RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: HUM-M01

‘Oh, Behave!’ A Global Outlook on Cyber Behaviors and the Science Behind

Oz Alashe MBE

CEO, CybSafe

ozalashe

Dr Jason R.C. Nurse

Associate Professor, University of Kent
Director of Science & Research, CybSafe

jasonrcnurse

Disclaimer

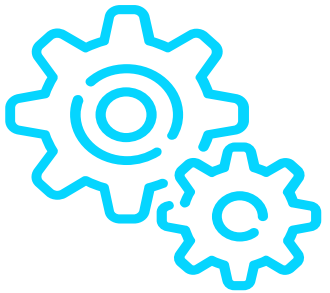
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The Annual Cybersecurity Attitudes and Behaviors report

Why?

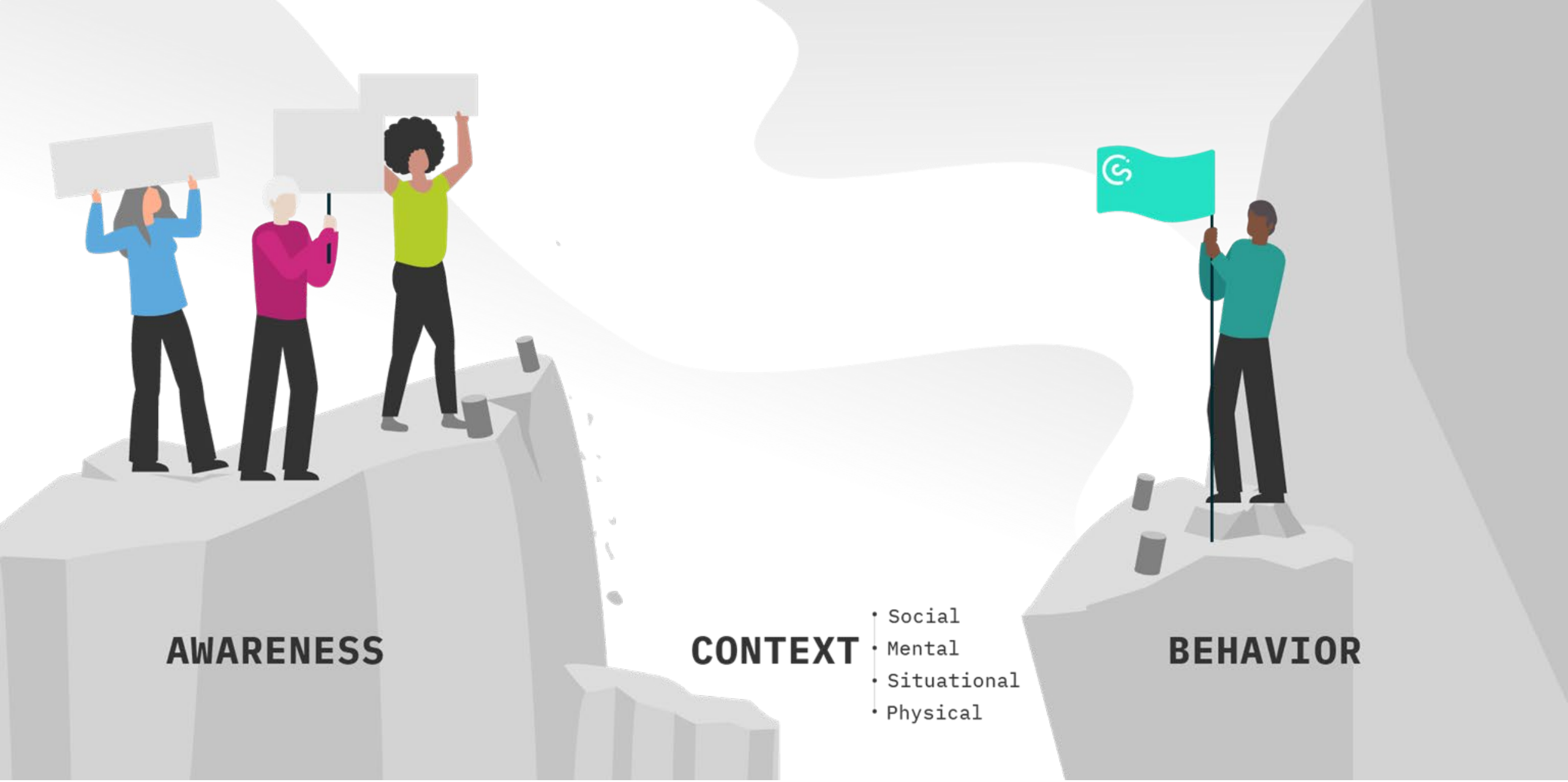


Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

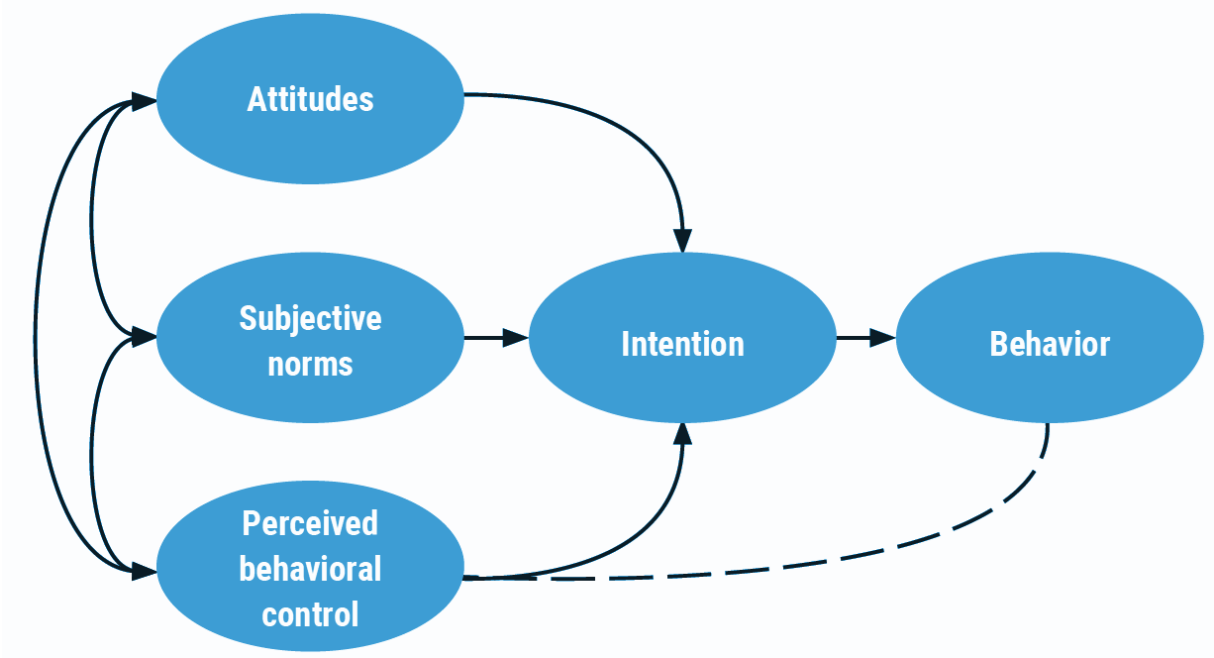
‘Everyone looked real’: multinational firm’s Hong Kong office loses HK$200 million after scammers stage deepfake video meeting

Biggest Deepfake Fraud? Fake Zoom Meeting, CFO Cloned, $25 Million Stolen

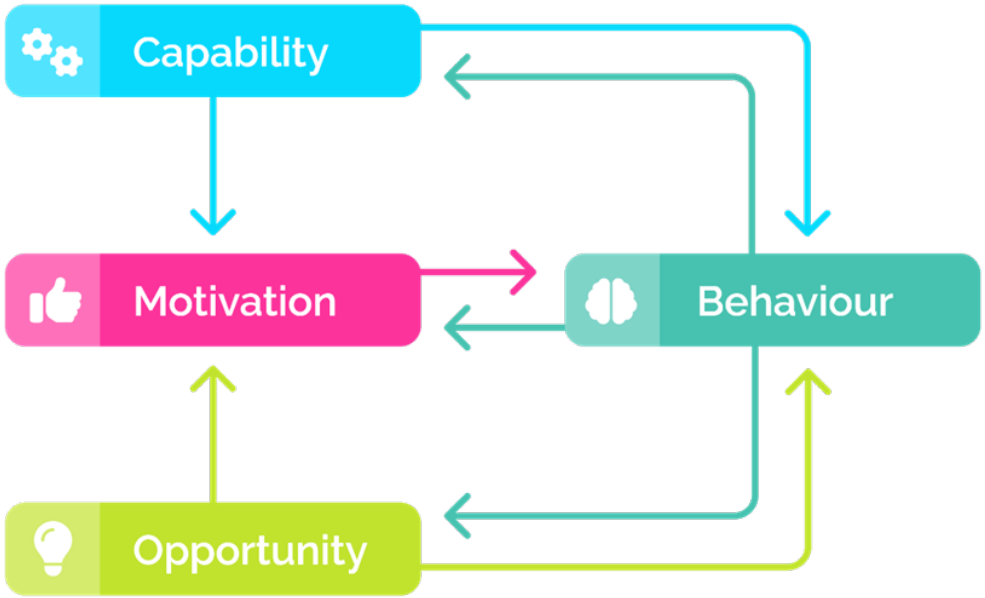
The company was manipulated through a multi-person video conference, where every participant, except the victim, was created using deepfake.


AWARENESS
CONTEXT
Social
Mental
Situational
Physical
BEHAVIOR

The psychology of behavior



Theory of Planned Behavior



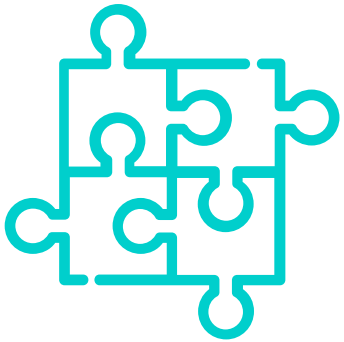
Capability, Opportunity, Motivation = Behavior (COM-B)

The psychology of behavior

The Knowledge-Attitude-Behavior (KAB) model

Knowledge affects **A**ttitude affects **B**ehavior

How?



Through?

Countries

- **US** 1000
- **Canada** 1000
- **UK** 1000
- **Germany** 1000
- **Australia** 1000
- **New Zealand** 1012
- **India** 1000

How?

Self-report survey

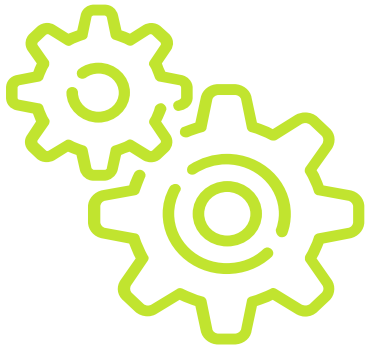
Who?

7012 participants (67% employed)

Age?

Gen Z (18-27)	15.8%
Millennials (28-43)	29.8%
Gen X (44-59)	28.3%
Baby Boomers (60-78)	24.6%
Silent Gen (79+)	1.5%

What?



Threat landscape:

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

Apple Joins A Growing List Of Companies Cracking Down On Use Of ChatGPT By Staffers—

Samsung Bans ChatGPT Among Employees After Sensitive Code Leak

Cybercrime reports:

FEDERAL BUREAU of INVESTIGATION
Internet Crime Report

';--have i been pwned?

Cyber security breaches survey 2024: technical report
Published 9 April 2024

Academic research:

nature reviews psychology

Explore content | About the journal | Publish with us | Subscribe

nature > nature reviews psychology > review articles > article

Review Article | Published: 03 May 2024

Determinants of behaviour and their efficacy as targets of behavioural change interventions

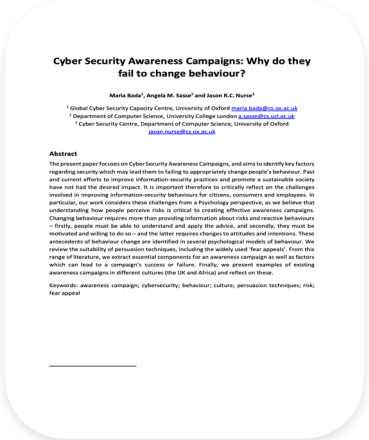
Dolores Albarracín, Bita Fayaz-Farkhad & Javier A. Granados Samayoa

Nature Reviews Psychology 3, 377–392 (2024) | Cite this article

20k Accesses | 8 Citations | 251 Altmetric | Metrics

Abstract

Unprecedented social, environmental, political and economic challenges — such as pandemics and epidemics, environmental degradation and community violence — require taking stock of how to promote behaviours that benefit individuals and society at large. In this Review, we synthesize multidisciplinary meta-analyses of the individual and social-structural determinants of behaviour (for example, beliefs and norms, respectively) and the efficacy of behavioural change interventions that target them. We find that, across domains, interventions designed to change individual determinants can be ordered by increasing impact as those targeting knowledge, general skills, general attitudes, beliefs, emotions, behavioural skills, behavioural attitudes and habits. Interventions designed to change social-structural determinants can be ordered by increasing impact as legal and administrative sanctions; programmes that increase institutional trustworthiness; interventions to change injunctive norms; monitors and reminders; descriptive norm interventions; material incentives; social support provision; and policies that increase access to a particular behaviour. We find similar patterns for health and environmental behavioural change specifically. Thus, policymakers should focus on interventions that enable individuals to circumvent obstacles to enacting desirable behaviours rather than targeting salient but ineffective determinants of behaviour such as knowledge and beliefs.


Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

Maria Bada[1], Angela M. Sasse[2] and Jason R.C. Nurse[3]

[1] Global Cyber Security Capacity Centre, University of Oxford maria.bada@cs.ox.ac.uk
[2] Department of Computer Science, University College London a.sasse@cs.ucl.ac.uk
[3] Cyber Security Centre, Department of Computer Science, University of Oxford jason.nurse@cs.ox.ac.uk

Abstract

The present paper focuses on Cyber Security Awareness Campaigns, and aims to identify key factors regarding security which may lead them to failing to appropriately change people's behaviour. Past and current efforts to improve information-security practices and promote a sustainable society have not had the desired impact. It is important therefore to critically reflect on the challenges involved in improving information-security behaviours for citizens, consumers and employees. In particular, our work considers these challenges from a Psychology perspective, as we believe that understanding how people perceive risks is critical to creating effective awareness campaigns. Changing behaviour requires more than providing information about risks and reactive behaviours – firstly, people must be able to understand and apply the advice, and secondly, they must be motivated and willing to do so – and the latter requires changes to attitudes and intentions. These antecedents of behaviour change are identified in several psychological models of behaviour. We review the suitability of persuasion techniques, including the widely used 'fear appeals'. From this range of literature, we extract essential components for an awareness campaign as well as factors which can lead to a campaign's success or failure. Finally, we present examples of existing awareness campaigns in different cultures (the UK and Africa) and reflect on these.

Keywords: awareness campaign; cybersecurity; behaviour; culture; persuasion techniques; risk; fear appeal

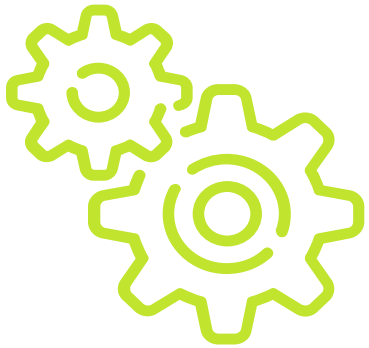
Cybersecurity topics

NATIONAL CYBERSECURITY ALLIANCE

National Cyber Security Centre

- Our online presence
- General attitudes to online security
- Reliance on others for cybersecurity
- Responsibility for cybersecurity
- Cybercrime victimization & reporting
- Cybersecurity training
- Cybersecurity knowledge & behaviors
  - Password hygiene
  - Enabling MFA
  - Installing software & app updates
  - Backing up data
  - Recognizing & reporting phishing messages
- Artificial Intelligence (AI)

Key findings



Attitudes

General attitudes

81%

consider online safety a priority

3% ↓ from 2023

60%

believe it's worth the effort

9% ↓ from 2023

53%

think staying safe online is possible

5% ↓ from 2023

46%

report staying safe online is frustrating

7% ↑ from 2023

44%

find it intimidating

7% ↑ from 2023

General attitudes

53%

think staying safe online is possible

5% ↓ from 2023

46%

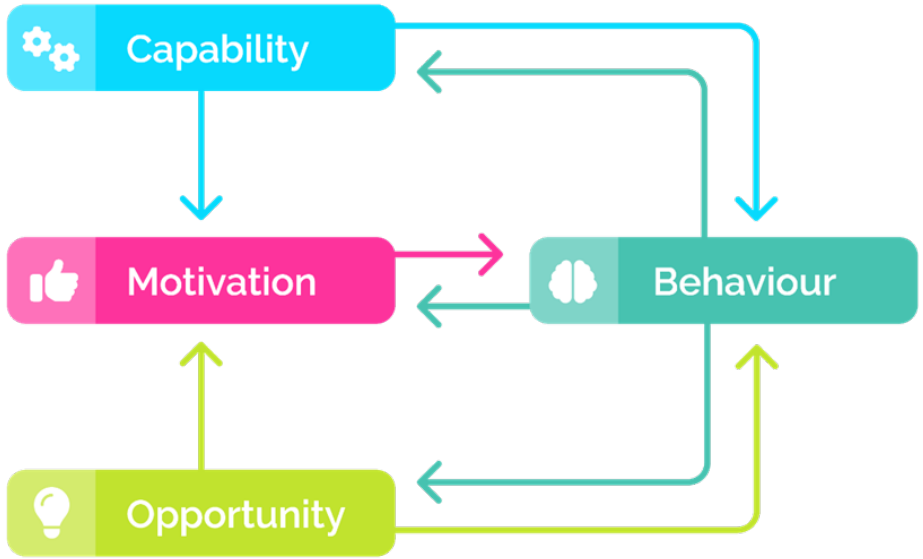
report staying safe online is frustrating

7% ↑ from 2023

44%

find it intimidating

7% ↑ from 2023



General attitudes: Country comparisons

Intimidating	Canada 49%, India 48%, USA 47%	vs	New Zealand 35%
Frustrating	USA 53%, Canada & Australia 52%	vs	Germany 37%
Possible	UK & New Zealand 61%	vs	Germany 45%
Under one's control	India 66%	vs	Germany 43%
Worth the effort	USA 59%, New Zealand 68%	vs	India 40%

Security (mis)conceptions

43%

"I presume my devices are **automatically secure**"

52%

"It is **expensive** to fully protect myself online"

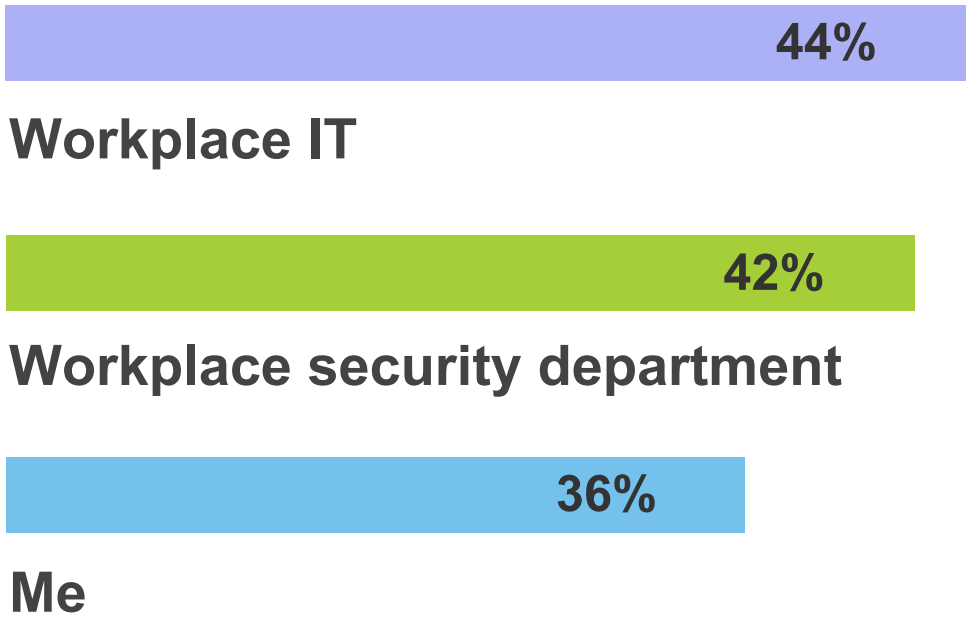
38%

Losing my personal details over the Internet **is unavoidable**!

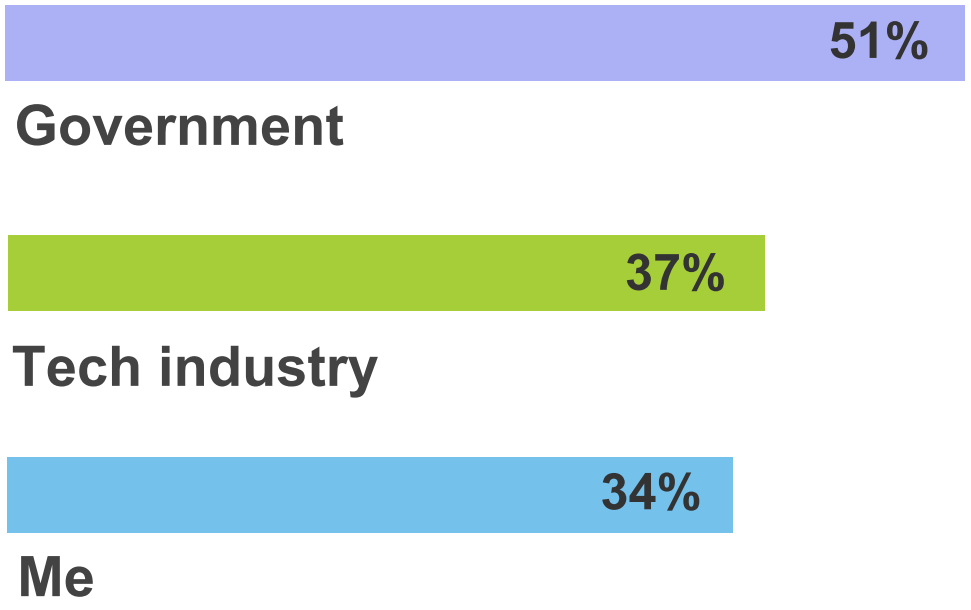
Learned helplessness *is a psychological phenomenon where an individual,* ***after repeatedly experiencing uncontrollable or aversive situations****, comes to believe that they have* ***no control over their circumstances****. As a result,* ***they stop trying to change or escape negative situations****, even when opportunities for change become available.*

Responsibility: Workplace information

Most responsible



Least responsible



Kingston

Cybersecurity training: Completion

86%*

are required to complete mandatory training

48%*

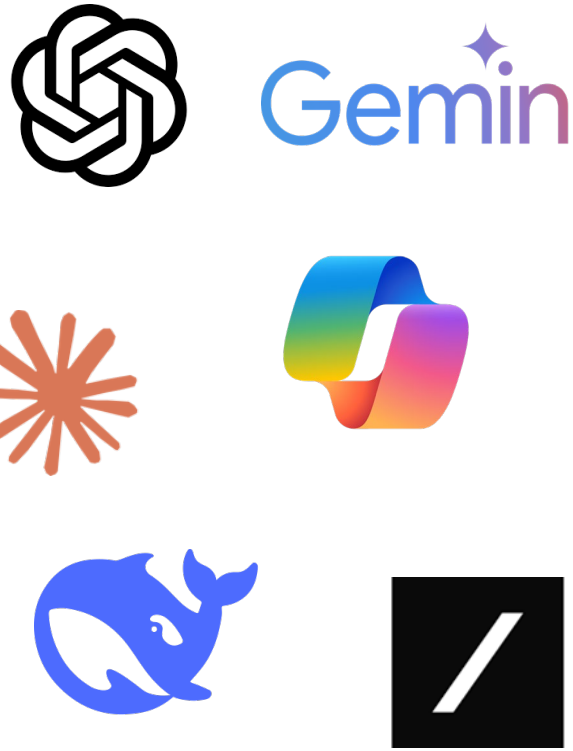
complete training once a year

17%

say they don't need cyber security information

* 86% (N=1432) of those with access to training at their workplace or place of education (N=1920)
* 48% (N=691) of those who are required to complete training (N=1432)

Cybersecurity training: AI



52%*

of employed participants have yet to receive any training on safe AI use

65%

expressed concern about AI-related cybercrime

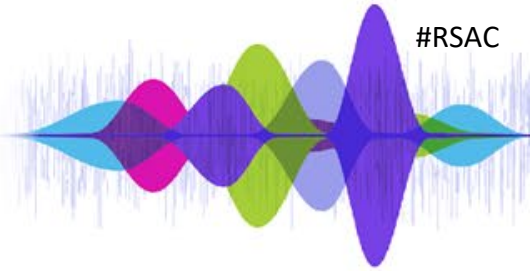
- **61%** of Gen X

vs

- **73%** of Silent Gen

* 52% (N=1340) of those who use AI tools (N=3087)

Cybersecurity training: What's your ideal format?



Video content	**Online courses held periodically**	**Written materials**	**Short, bite-sized pieces of information**	**Online games or gamified experiences**

Cybersecurity training: Preferences

46%

Video content

27% of Gen Z

26% of Millennials

24% of Gen X

37%

Online courses held periodically

35%

Written materials

36% Silent Gen

25% Baby Boomers

33%

Short, bite-sized pieces of information

11%

Online games or gamified experiences

Training: Preferred format (country comparisons)

Video content

USA 26% | Canada | New Zealand | India 25%

Australia 24% | UK 23%

Written materials

Germany 24%

Online courses

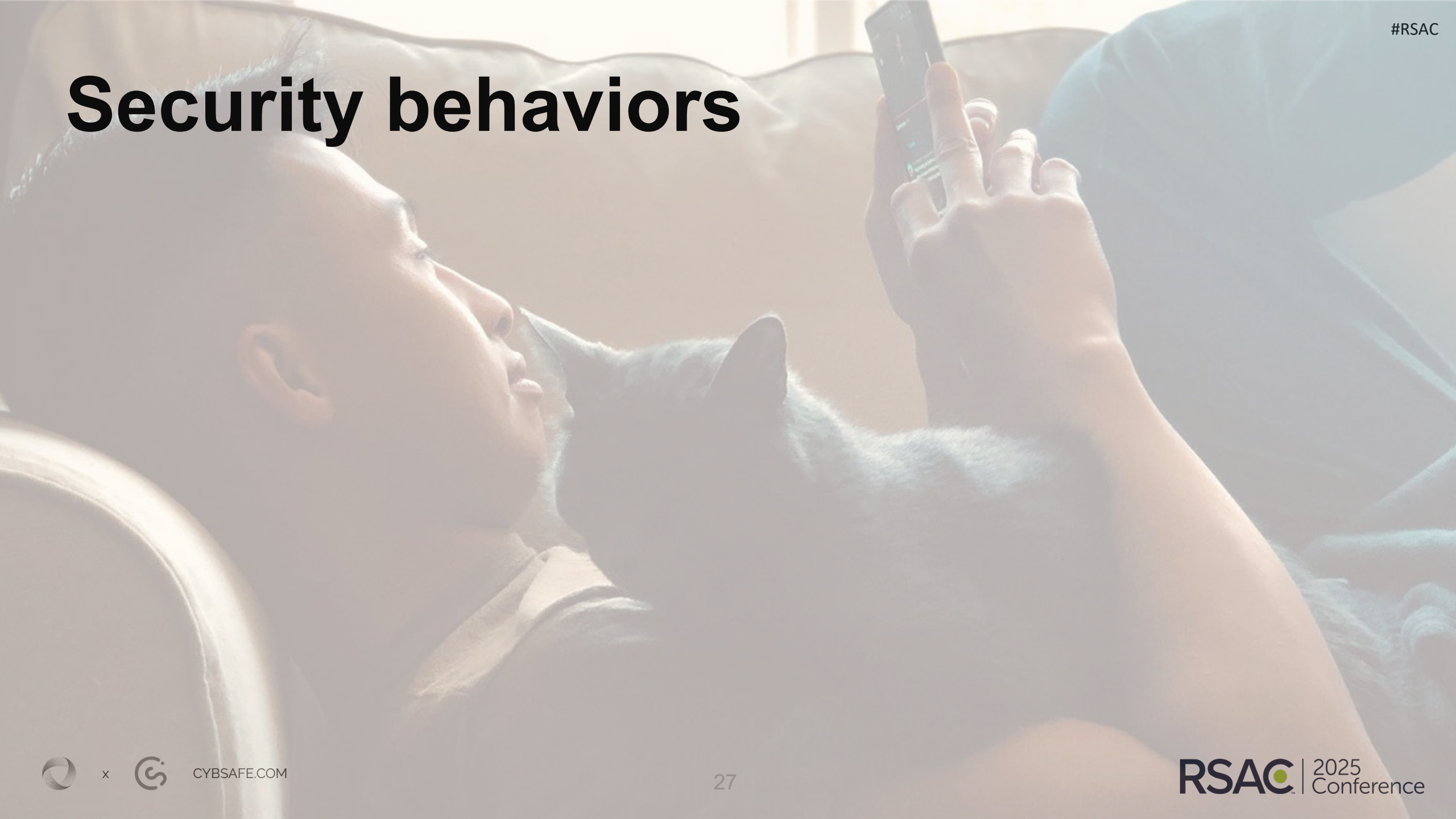
UK 23%

Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

Maria Bada[1], Angela M. Sasse[2] and Jason R.C. Nurse[3]

[1] Global Cyber Security Capacity Centre, University of Oxford maria.bada@cs.ox.ac.uk
[2] Department of Computer Science, University College London a.sasse@cs.ucl.ac.uk
[3] Cyber Security Centre, Department of Computer Science, University of Oxford
jason.nurse@cs.ox.ac.uk

Security behaviors



Artificial Intelligence (AI)

38%*

shared sensitive work information with AI without their employer's knowledge

- **46%** of Gen Z **vs**
- **14%** of Baby Boomers

AI Improves Employee Productivity by 66%

Stanford and MIT study: A.I. boosted worker productivity by 14%—those who use it 'will replace those who don't'

Apple said AI could lead to a potential leak of confidential data

* 38% (N=733) of those who use AI tools for work (N=1920)

Artificial Intelligence (AI)

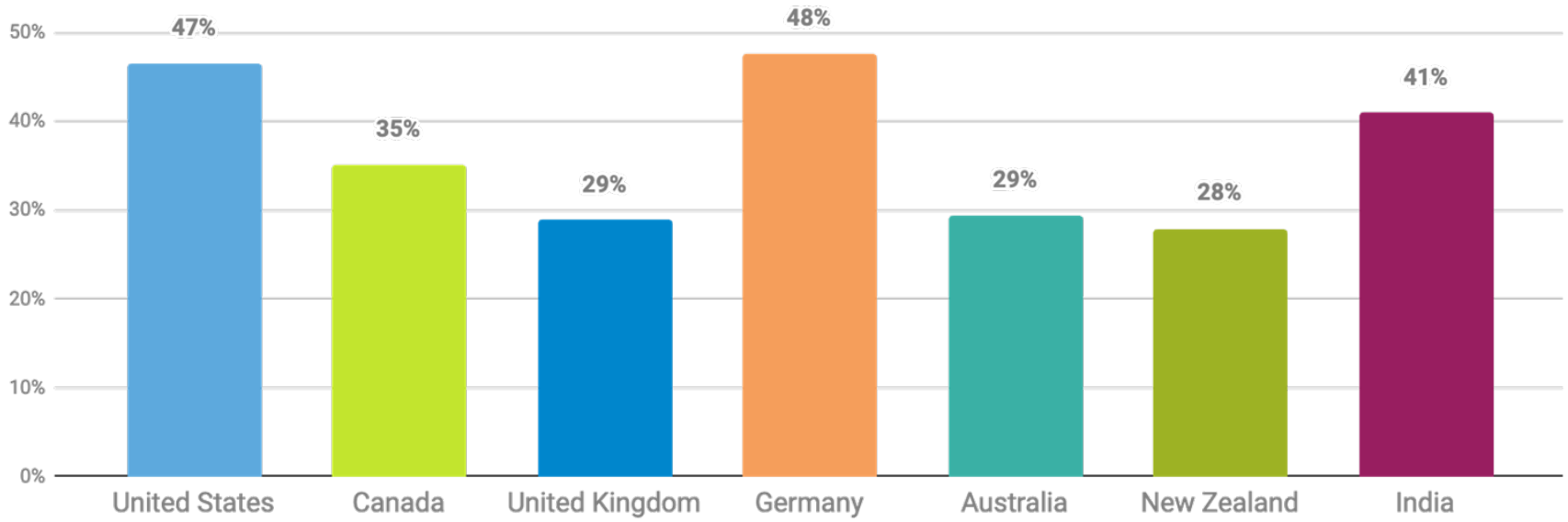
38%*

shared sensitive work information with AI without their employer's knowledge

- **46%** of Gen Z

vs

- **14%** of Baby Boomers



* 38% (N=733) of those who use AI tools for work (N=1920)

Passwords

Log On to Windows
Microsoft
Windows 2000
Professional
Built on NT Technology
Microsoft
User name:
Admin
Password:
Log on using dial-up connection
OK
Cancel
Shutdown...
Options <<

Log On to Windows
Microsoft
Windows xp
Professional
Copyright © 1985-2001
Microsoft Corporation
Microsoft
User name:
Administrator
Password:
OK
Cancel
Options >>

What's the best password?

1. laptopgrassplastic1*
2. ab!3z9RpdE
3. pa$$w0rd_rsac25

Password hygiene

78%

know how to create strong passwords and do so

- **84%** of Baby Boomers
vs
- **70%** of Gen Z

35%

include personal information in their passwords

- **52%** of Gen Z
vs
- **21%** of Baby Boomers

32%

create shorter than 9-character passwords

- **30%** of Gen Z
vs
- **32%** of Baby Boomers & Silent Gen

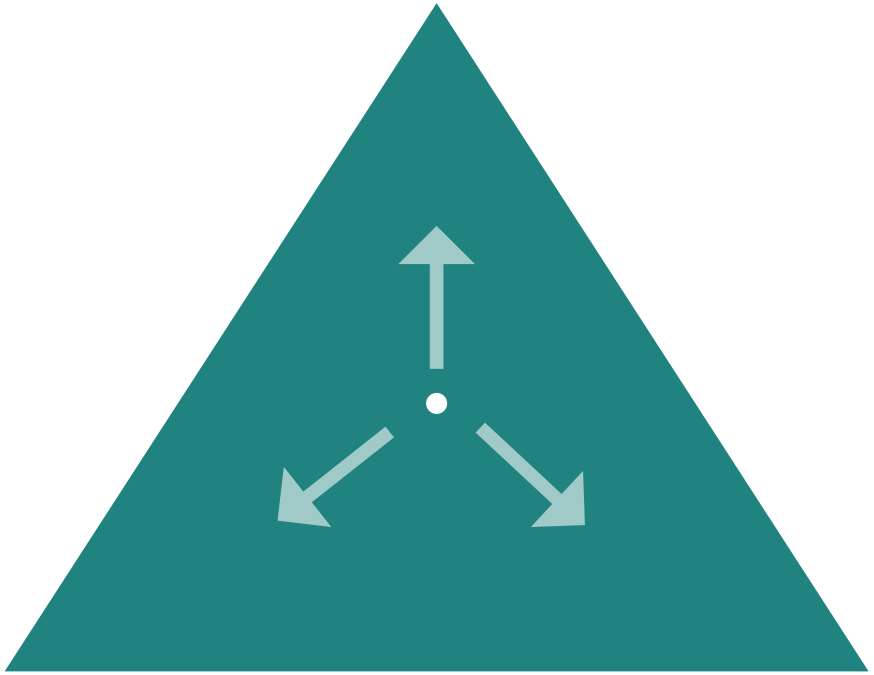
40%

create passwords using a single dictionary word or someone's name

- **52%** of Gen Z
vs
- **28%** of Silent Gen

Password hygiene

Security



Functionality

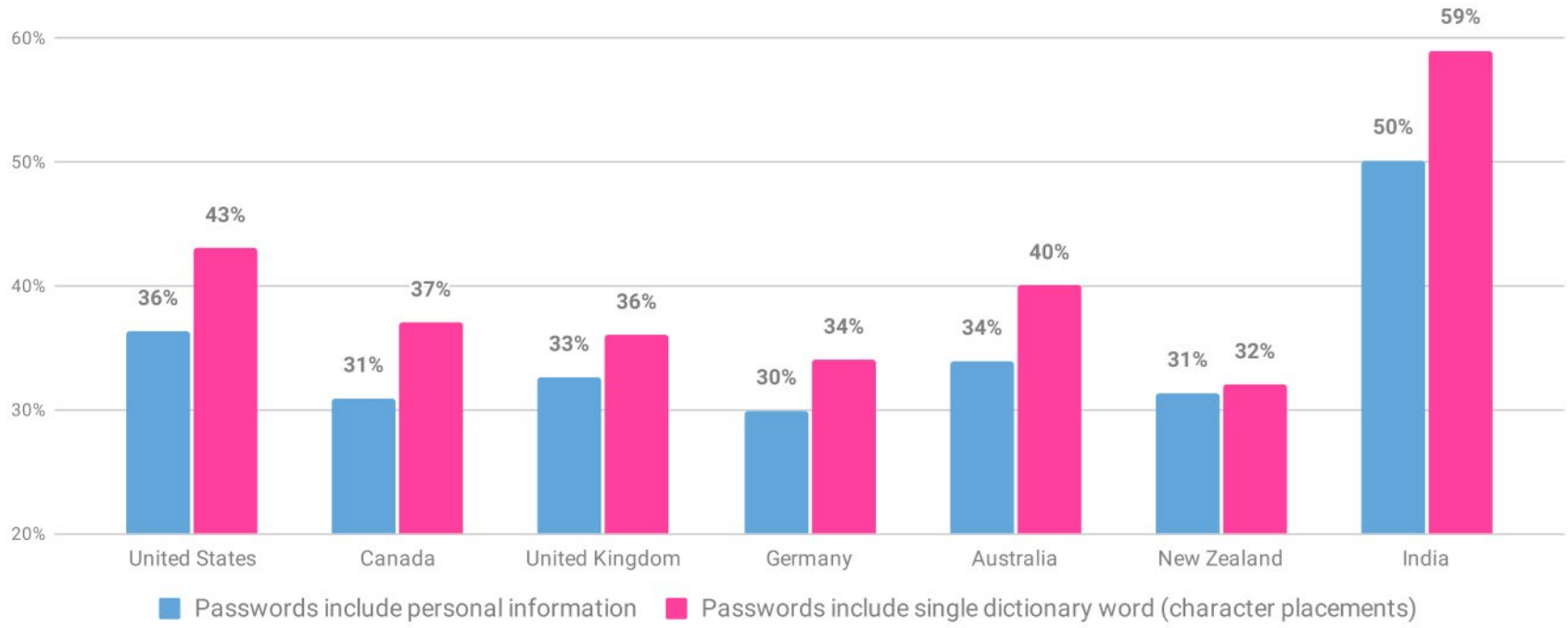
Usability

Password hygiene

35%

include personal information in their passwords

- **52%** of Gen Z **vs**
- **21%** of Baby Boomers



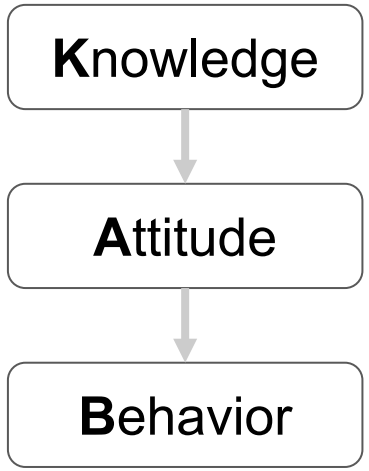
Multi-factor authentication

81% have heard of MFA.
- ***87%*** *of Millennials* ***vs*** ***51%*** *of Silent Gen*

66% of those reported knowing how to, and using it.
- ***71%*** *of Baby Boomers and* ***70%*** *of Gen X* ***vs*** ***56%*** *of Gen Z*

24% either don't or stopped using it despite knowing how to.
- ***35%*** *of Gen Z* ***vs*** ***16%*** *of Silent Gen*

"It [MFA] annoys the heck out of me!!" **PS8424, Canada**



Phishing

67%

always or very often check the legitimacy of messages

- **78%** of Baby Boomers **vs** **55%** of Gen Z

47%

always or very often report phishing

- **54%** of Gen Z **vs**
- **25%** of Silent Gen

Of those who don't report phishing:

71% would do so if it helped to stop cybercriminals

68% would do so if it would stop spam messages from getting into their inbox

60% would do so if something would happen as a result

*"I receive spam and fraud emails at least once a week. … Sometimes I report them but **I don't know if anyone does anything about them**."* **PS8811, Canada**

Training: Barriers to engagement

Of those who don't complete security awareness training:

23% "already know enough"
(**5%** ↑ from 2023)

22% 22% cite a *lack of time*
(**7%** ↓ from 2023)

20% don't believe it will *reduce their risk of cybercrime*
(**4%** ↑ from 2023)

"Informing oneself is more effective [than attending a cybersecurity training course]."

PS7967 Germany

"I don't do any cybersecurity training, just use my own common sense."

PS290, New Zealand

The psychology of behavior

The Knowledge-Attitude-Behavior (KAB) model

Knowledge affects **A**ttitude affects **B**ehavior

Call to action!

- **Next week, you should:**
  - Review your approach to the human element of cybersecurity; to what extent is it based on science and setup to facilitate real behavior change?
- **In the first three months, you should:**
  - Consider that people's knowledge, attitudes and motivations influence their security behaviors; not just knowledge (training) alone.
  - Help people use AI in safe, secure, and responsible ways.
- **Within six months, you should:**
  - Define an approach to the human element of cybersecurity that is grounded in science and appreciates the needs of different age groups, countries and cultures.

RSAC 2025 Conference

Oz Alashe MBE

Dr Jason R.C. Nurse

Thanks for attending!

Any questions?

Many Voices.
One Community.